FortiSandbox™

Multi-layer proactive threat mitigation

Today's most sophisticated cybercriminals are increasingly bypassing traditional antimalware solutions and inserting advanced persistent threats deep within networks. These highly targeted attacks evade established signature-based detection by masking their malicious nature in many ways — compression, encryption, polymorphism, the list of techniques goes on. Some have even begun to evade virtual "sandbox" environments using VM detection, "time bombs" and more. Fighting today's attacks requires a comprehensive and integrated approach — more than antimalware. More than a virtual sandbox. More than a separate monitoring system.

FortiSandbox offers a robust combination of proactive detection and mitigation, actionable threat insight and easy, integrated deployment. At its foundation is a unique, dual-level sandbox which is complemented by Fortinet's award-winning antimalware and optional integrated FortiGuard threat intelligence. Years of Fortinet threat expertise is now packaged up and available on site via FortiSandbox.

Proactive Detection and Mitigation

Suspicious codes are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. The highly effective pre-filters include a screen by our AV engine, queries to cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime environment. Once a malicious code is detected, results are submitted for antimalware signature creation as well as updates to other threat databases.

Actionable Insight

All classifications — malicious and high/medium/low risk — are presented within an intuitive dashboard. Full threat information from the virtual execution — including system activity, exploit efforts, web traffic, subsequent downloads, communication attempts and more — is available in rich logs and reports.

Easy Deployment

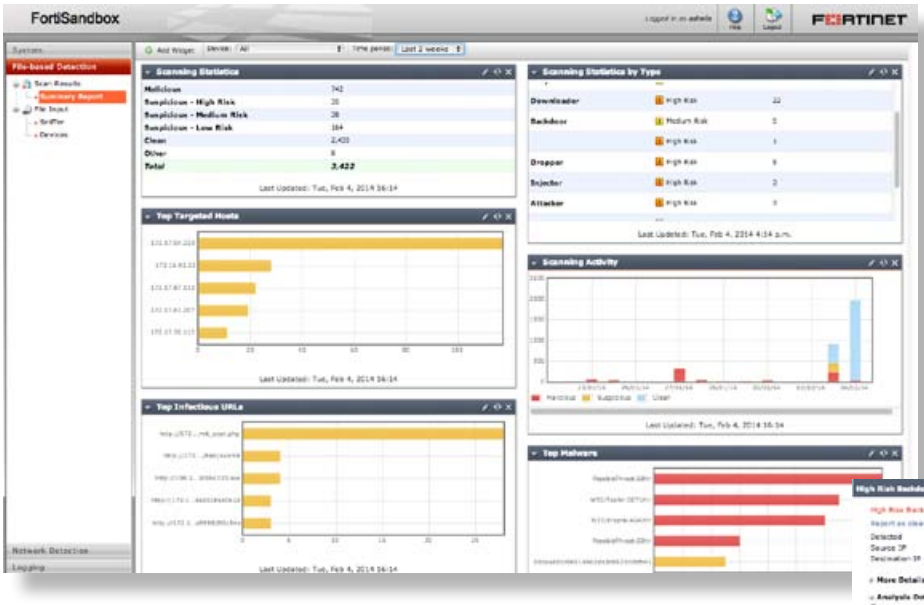
FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates with FortiGate as a new capability within your existing security framework.

The ultimate combination of proactive mitigation, advanced threat visibility and comprehensive reporting.

- Secure virtual runtime environment exposes unknown threats
- Unique multi-layer pre-filters for fast and effective threat detection
- Rich reporting for full threat lifecycle visibility
- Inspection of many protocols in one appliance simplifies deployment and reduces cost
- Integration with FortiGate enhances rather than duplicates security infrastructure
- Validated security with NSS BDS (Breach Detection Systems) testing

NSS LABS RECOMMEND

FEATURES

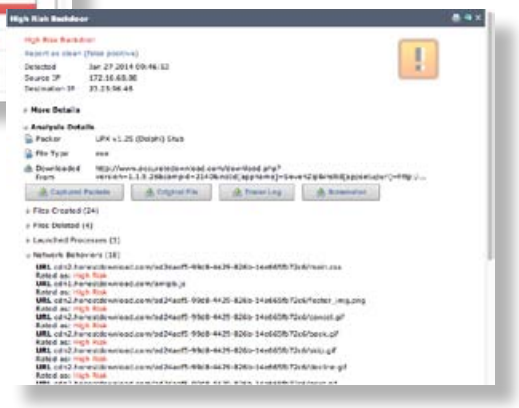


Dashboard Widgets — Real-time threat status

VM Sandboxing

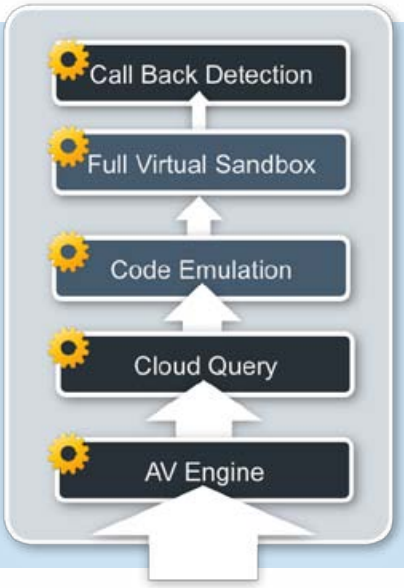
Complement your established defenses with cutting-edge capability — analyzing suspicious and high-risk files in a contained environment to uncover the full attack lifecycle using system activity and callback detection.

Detailed File Analysis Report



File Analysis Tools

Reports with captured packets, original file, tracer log and screenshot provide rich threat intelligence and actionable insight after files are examined. This is to speed up remediation and updated protection.



Multi-tiered file processing optimizes resource usage that improves security, capacity and performance

AV Engine

- Applies top-rated (95%+ Reactive and Proactive) AV Scanning. Serves as an efficient pre-filter.

Cloud Query

- Real-time check of latest malware information
- Access to shared information for instant malware detection

Code Emulation

- Quickly simulates intended activity
- OS independent and immune to evasion/obfuscation

Full Virtual Sandbox

- Secure run-time environment for behavioral analysis/rating
- Exposes full threat lifecycle information

Call Back Detection

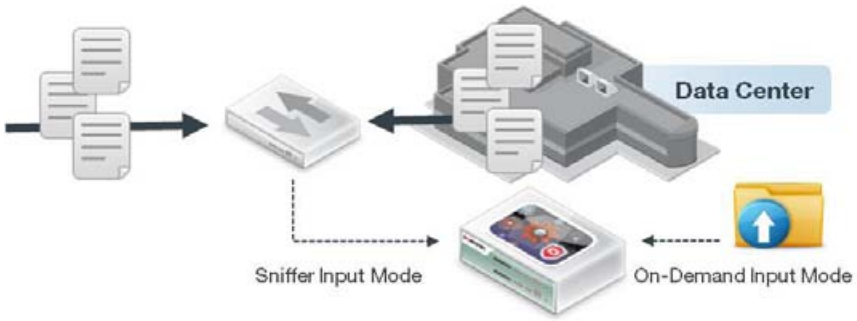
- Identifies the ultimate aim, call back and exfiltration

DEPLOYMENT OPTIONS

The FortiSandbox is the most flexible threat analysis appliance in the market as it offers various deployment options for customers' unique configurations and requirements. Organizations can also have all three input options at the same time.

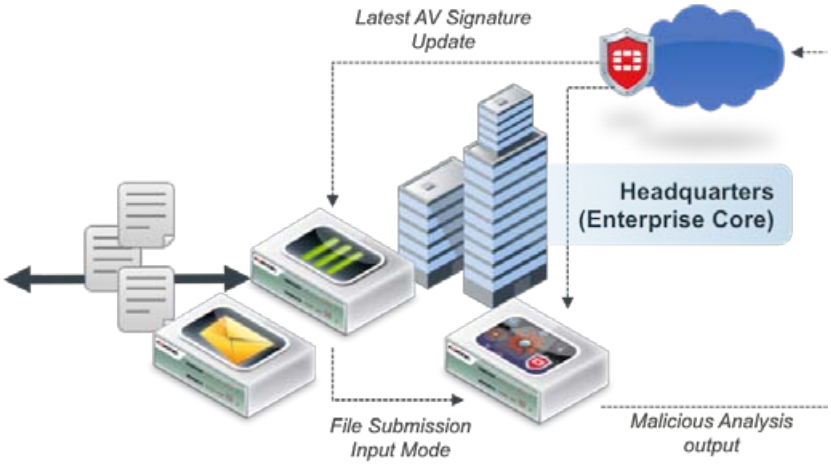
Standalone

This deployment mode relies on inputs from spanned switch ports and/or administrators' on-demand file uploads using the GUI. It is the most suitable infrastructure for adding protection capabilities to existing threat protection systems from various vendors.



*FortiGate/FortiMail Integrated

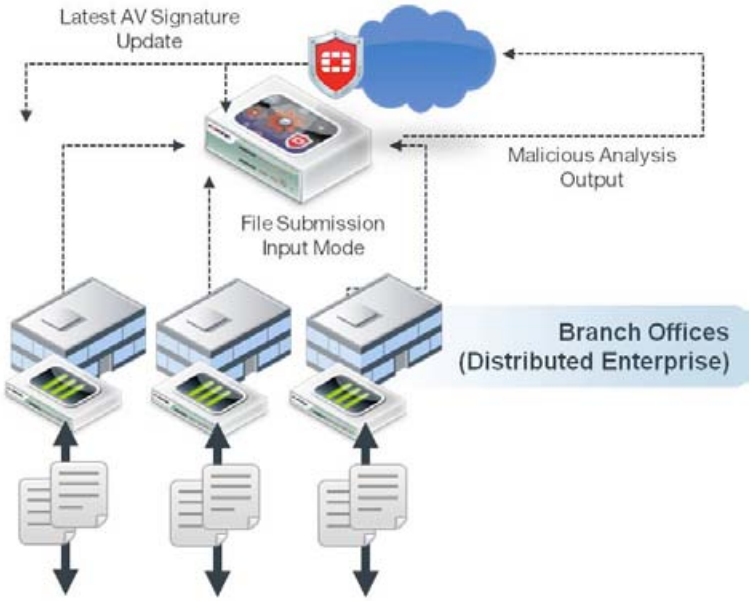
The FortiGate, as the Internet security gateway, can be set up to submit suspicious files to the FortiSandbox. This seamless integration reduces network complexity and expands the applications and protocols supported including SSL encrypted ones such as HTTPS.



* Requires: FortiOS V5.0.4+, FortiMail V5.1+

Distributed FortiGate Integrated

This deployment is attractive for organizations that have distributed environments, where FortiGates are deployed in the branch offices and submit suspicious files to a centrally-located FortiSandbox. This setup yields the benefits of lowest TCO and protects against threats in remote locations.



FEATURES SUMMARY

Administration

Supports WebUI and CLI configurations

Multiple administrator account creation

Configuration file backup and restore

Notification email when malicious file is detected

Weekly report to global email list and FortiGate administrators

Frequent signature auto-updates

VM status monitoring

Networking/Deployment

Static Routing Support

File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)

Device Integration:
- File Submission input: FortiGate (V5.0.4+), FortiMail (5.1.0+ ??)
- Update Database host: FortiManager (V5.0.6+)

Advanced Threat Protection

Virtual OS Sandbox:
- Concurrent Windows instances
- Anti-evasion techniques: sleep calls, process and registry queries
- Callback Detection: malicious URL visit, Botnet C&C communication and Attacker traffic from activated malware
- Download Capture packets, Original File, Tracer log and Screenshot

Unlimited file size support, maximum file size configurable

File type support:
- Archived: .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj
- Executable files (eg: .exe, .dll), PDF, Windows Office Document and Javascript
- Media files: .avi, .mpeg, .mp3, .mp4

Protocols/applications supported:
- Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
- Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL encrypted versions
- Integrated mode with FortiMail: SMTP, POP3, IMAP

Network Threat Detection in Sniffer Mode: Identify Botnet activties and network attacks, malicious URL visit

Option to auto-submit suspicious files to cloud service for manual analysis and signature creation

Monitoring and Report

Real-Time Monitoring Widgets (viewable by source and time period options): Scanning Result statistics, Scanning Activities (over time), Top Targeted Hosts, Top Malware, Top Infectious URLs, Top Callback Domains

Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time and download path

Logging — GUI, download RAW log file

Report generation for malicious files: Detailed reports on file characteristics and behaviors – File Modification, Process Behaviors, Registry Behaviors, Network Behaviors, VM snapshot

Further Analysis: Downloadable files — Sample file, Sandbox tracer logs and PCAP capture

SPECIFICATIONS

	FSA-1000D	FSA-3000D
Hardware		
Form Factor	2 RU	2 RU
Total Network Interfaces	6x GE RJ45 ports, 2x GE SFP slots	4x GE RJ45 ports, 2x GE SFP slots
Storage Capacity	4 TB (max. 8 TB)	8 TB (max. 16 TB)
Power Supplies	2x Redundant PSU	2x Redundant PSU
System		
VM Sandboxing (Files/Hour)	160	560
AV Scanning (Files/Hour)	6,000	15,000
Number of VMs	8	28
Dimensions		
Height x Width x Length (in)	3.5 x 17.2 x 14.5	3.3 x 19.0 x 29.7
Height x Width x Length (mm)	89 x 437 x 368	84 x 482 x 755
Weight	27.60 lbs (12.52 kg)	71.5 lbs (32.5 kg)

	FSA-1000D	FSA-3000D
Environment		
Power Consumption (AVG / MAX)	115 / 138 W	392 / 614.6 W
Maximum Current	100V/5A, 240V/3A	110V/10A, 220V/5A
Heat Dissipation	471 BTU/h	2131.14 BTU/h
Power Source	100–240 VAC, 60–50 Hz	100–240 VAC, 60–50 Hz
Humidity	5–95% non-condensing	20–90% non-condensing
Operation Temperature Range	32–104°F (0–40°C)	50–95°F (10–35°C)
Storage Temperature Range	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)
Compliance		
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	

ORDER INFORMATION

Product	SKU	Description
FortiSandbox-1000D	FSA-1000D	Advanced Threat Protection System — 6x GE RJ45, 2x GE SFP slots, redundant PSU, 6 Windows XP licenses and 2 Windows 7 licenses included.
FortiSandbox-3000D	FSA-3000D	Advanced Threat Protection System — 4x GE RJ45, 2x GE SFP slots, redundant PSU, 22 Windows XP licenses and 6 Windows 7 licenses included.
Optional Accessories	**SKU**	**Description**
SFP SX Transceiver Module	FG-TRAN-SX	Transceiver SX module for models with SFP interfaces.
SFP LX Transceiver Module	FG-TRAN-LX	Transceiver LX module for models with SFP interfaces.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480